IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

THE TRUSTEES OF COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK, *Plaintiff*, v. SYMANTEC CORPORATION, *Defendant*.	Civil Action No. 3:13-cv-00808-MHL

PLAINTIFF'S MEMORANDUM IN OPPOSITION TO DEFENDANT'S MOTION FOR JUDGMENT ON THE PLEADINGS PURSUANT TO FED. R. CIV. P. 12(c) AND 35 U.S.C. § 101

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTE

OTHER AUTHORITIES

Plaintiff, The Trustees of Columbia University in the City of New York ("Columbia"), submits this memorandum in opposition to Defendant Symantec Corporation's ("Symantec") motion for judgment on the pleadings, which asserts that the claims of the patents in suit, U.S. Patent Nos. 8,074,115 (the "'115 patent") and 8,601,322 (the "'322 patent"), are invalid under 35 U.S.C. § 101. Dkt. No. 245.

I. PRELIMINARY STATEMENT

Symantec's motion is premised on ignoring an established line of cases in the Federal Circuit holding that patent claims that improve computer functionality—as claims asserted in the '115 and '322 patents (the "Asserted Claims") undeniably do—are valid under § 101. (*See infra* pp. 11–16.) Only by ignoring this precedent, which found claims indistinguishable from those at issue here patentable, and by improperly construing the Asserted Claims to a level of abstraction that makes the claims virtually unrecognizable, can Symantec contend the asserted claims are invalid. The Asserted Claims are carried out on millions of computers running Symantec products to prevent malware from being successful; the claimed inventions are not "abstract" ideas. Because Symantec's motion is without merit when viewed through this controlling law (which Symantec does not even address), its motion should be summarily denied.

The timing of Symantec's Rule 12(c) motion, made almost six years after the amended complaint and answer were filed, suggests yet another effort to avoid trial. Symantec offers no explanation for why its motion was not raised in 2014 before this case was stayed and appealed to the Federal Circuit, or why the motion was not even mentioned during the October 4, 2018 conference with the Court so it could be efficiently addressed at the November 27, 2018 hearing. As the Court noted at the November 27, 2018 hearing: "[P]art of what you [Symantec] say is it would have been ridiculous, or ludicrous . . . to raise [additional arguments] then [before Judge Spencer], but why is it not more ludicrous to take it up two appellate reviews and come back and raise it now? Why is that not more ludicrous?" Dkt. No. 234 at 62. The same point applies here. Symantec's tardy motion borders on the frivolous and should be denied.[1]

In order to determine patent-eligibility under § 101, the Supreme Court has established a two-step analysis. At step one, courts determine whether the claims at issue are "directed to" a patent-ineligible concept, such as an abstract idea. If so, at the second step the court searches for an "inventive concept" sufficient to transform the abstract idea into a patent-eligible application.

With respect to the first step, Symantec's contention that the Asserted Claims are directed to an abstract idea is based on ignoring the closest § 101 precedent and a misreading and oversimplification of those claims such that the key features that render them patentable are obscured or eliminated. Indeed, Symantec entirely ignores the Federal Circuit's controlling decision in *Finjan, Inc.* v. *Blue Coat Systems, Inc.*, 879 F.3d 1299 (Fed. Cir. 2018). In *Finjan*, the Federal Circuit considered patent claims directed to malware detection, like the Asserted Claims, and held the claims patent-eligible because they improved computer functioning. Symantec's failure to address *Finjan* is striking given that Symantec, who acquired Blue Coat in 2016, was the defendant/appellee in that case (and ultimately settled the case for $65 million). Instead of addressing the governing Federal Circuit cases, Symantec relies entirely on cases that the Federal Circuit has repeatedly held to be inapplicable to claims such as the Asserted Claims—those directed to improvements to computer functionality.

Although the Court need not proceed to the second step of the Supreme Court's § 101 analysis, the Asserted Claims are patentable under that standard. At least two of the key

[1] District courts hold "broad discretion . . . in managing [their] docket[s]," *see Great Am. Ins.* v. *Gross*, No. 3:05-cv-159, 2007 WL 1577503, at *13 (E.D. Va. May 30, 2007) (Lauck, J.). As noted in Rule 12(c) Symantec's motion should not be permitted to delay any trial schedule.

claim elements—the "model of function calls" element, where the model is selected randomly from multiple models or created by combining models, and the "application community" element—viewed individually, or as an ordered combination, present "inventive concepts" sufficient to satisfy step two. Each of these claim elements offers substantially more than required to meet the relevant inquiry: whether the claim element was well-understood, routine, and conventional. At the very least, the patents and their specifications raise questions of material fact that make judgment on the pleadings improper under *Berkheimer* v. *HP Inc.*, 881 F.3d 1360 (Fed. Cir. 2018) (whether claims are well-understood, routine, and conventional may be questions of fact for the jury).

II. STATEMENT OF FACTS

A. The '115 and '322 Patents

The '115 and '322 patents—developed jointly by Professor Salvatore Stolfo and Professor Angelos Keromytis at Columbia University's Intrusion Detection Systems Laboratory and Network Security Laboratory and entitled "Methods, Media and Systems for Detecting Anomalous Program Executions"—disclose innovations in computer security software for detecting anomalous behavior in running programs caused by viruses or other malware. *See* '322 patent at 1:19–20. As the common specification of these patents describes, the nature and type of "function calls"—the requests made by programs to link to and use subroutines in a computer to carry out user instructions—can be a leading indicator of intrusions or attacks. *Id.* at 3:28–56. Accordingly, "instrumenting, monitoring, and analyzing application-level program function calls and/or arguments . . . can be used to detect anomalous program executions that may be indicative of a malicious attack or program fault." *Id.* at 3:7–15.

The inventions of the '115 and '322 patents share several common features, including: (1) running at least a part of the program being monitored for malware in an "emulator";

(2) comparing one or more of the function calls made by the program in the emulator to a "model of function calls"; (3) identifying "anomalous" function calls based on comparison with the model; and (4) notifying an "application community" of the anomalous function call. *See, e.g.*, *id.* at 2:20–26, 6:31–33. Importantly, the Asserted Claims require that the "model[s] of function calls" be selected or updated in ways that impede malware creators from designing around them. *See, e.g.*, *id.* at 6:48–51, 6:55–57.

Claims 2, 9, 10, and 23 of the '115 patent and claims 2 and 8 of the '322 patent are a good starting point.[2] Claim 2 of the '115 patent depends on (*i.e.*, incorporates all of the limitations of) claim 1, which reads:

1. A **method** for detecting anomalous program executions, comprising:
executing at least a part of a program in an **emulator**;
comparing a function call made in the emulator to **a model of function calls for the at least a part of the program**;
identifying the function call as **anomalous** based on the comparison; and
upon identifying the anomalous function call, **notifying an application community** that includes a plurality of computers of the anomalous function call.

Claim 2 adds the limitation of "creating a combined model from at least two models created using different computers." '115 patent at 20:47–49. Similarly, claims 9 and 10 also depend on claim 1, but add the limitations of "randomly selecting the model as to be used in the comparison from a plurality of different models relating to the program" and "randomly selecting a portion of the model to be used in the comparison," respectively. *Id.* at 20:65–21:2.

Claim 23 of the '115 patent depends on claim 22, which reads:

22. A **method** for detecting anomalous program executions, comprising:

[2] Columbia asserts that Symantec infringes claims 2, 9, 10, 12, 19, 20, 23, 30, 31, 33, 40, and 41 of the '115 patent, and claims 2, 8, 11, 17, 25, and 27 of the '322 patent (the "Asserted Claims"). For purposes of the § 101 analysis, there are no relevant differences between the claims discussed above and the other Asserted Claims.

modifying a program to include **indicators of program-level function calls** being made during execution of the program;
comparing at least one of the indicators of program-level function calls made in an **emulator** to a **model of function calls for at least a part of the program**; and
identifying a function call corresponding to the at least one of the indicators as **anomalous** based on the comparison.

Claim 23 adds the limitation of "creating a combined model from at least two models created using different computers." *Id.* at 21:60–62.

Claim 2 of the '322 patent reads:

2. A **method** for detecting anomalous program executions, comprising:
executing at least a portion of a program in an **emulator**;
comparing a function call made in the emulator to a **model of function calls for the at least a portion of the program**,
wherein the model is a **combined model** created from at least two models **created using different computers**; and
identifying the function call as **anomalous** based on the comparison.

And claim 8 of the '322 patent depends on claim 1, which reads:

1. A **method** for detecting anomalous program executions, comprising:
executing at least a portion of a program in an **emulator**;
comparing a function call made in the emulator to a **model of function calls for the at least a portion of the program**,
wherein the model is a combined model created from at least two models **created at different times**; and
identifying the function call as **anomalous** based on the comparison.

Claim 8 adds the limitation of "**randomly selecting at least a portion of the model** to be used in the comparison from a plurality of different models relating to the program." '322 patent at 21:1–4 (emphasis added).

As the shared specification explains, computers have traditionally been protected by "antivirus software" that may use static or "fingerprint" analysis to detect and prohibit the execution of previously identified viruses. These "static" detections recognize a unique pattern of characters—a "signature"—indicative of malicious code, which is only possible if that signature has been previously identified. *See Finjan*, 879 F.3d at 1304, 1311 (describing a similar technical problem in the context of the patented technology in that case). But static detection is "not always adequate" to defend against many types of malware, including "remote attacks, high volume events (such as fast-spreading worms like Slammer and Blaster), or simple application-level denial of service (DoS) attacks." '322 patent at 1:32–37. Notably, traditional antivirus software cannot detect attacks that have never been seen before, known as "zero day" attacks.

The inventions of the '115 and '322 patents address this detection problem by relying on sophisticated and dynamic analysis of program behavior, rather than a static analysis of its code. In particular, the patented inventions detect attacks by identifying "anomalous" behavior (indicative of malware) through a comparison of actual program behavior (via "function calls") against a "model" of function calls.[3]

All of the Asserted Claims require a "model of function calls for the at least a part [or portion] of the program." *E.g.*, '115 patent at claims 2, 9, 10; '322 patent at claims 2, 8. The common specification teaches that the model of function calls is developed from data collected from analyzing function calls made during typical program execution, which may include "attack" as well as "attack-free" data. *See* '322 patent at 3:46–56 ("an anomaly detector models normal program execution stack behavior"); *id.* at 3:34–45 (The execution of programs is monitored to extract "indicators of what function[] calls are being made" and "other suitable related

[3] Contrary to Symantec's claim that "nothing in the claims specifies what constitutes an anomaly," Dkt. No. 246 ("Symantec Br.") at 5, this Court previously construed the term "anomalous," at Symantec's request, to mean "[d]eviation/deviating from a model of typical, attack-free computer system usage." Claim Construction Order, Dkt. No. 123. The Federal Circuit subsequently vacated the "attack-free" aspect of the construction, and Columbia contends that the term should thus be construed to mean "[d]eviation/deviating from a model of typical computer system usage." Dkt. No. 213 at 7. Symantec now asks that the Court reject its original construction in its entirety and re-construe the term to mean "deviating from normal." Dkt. No. 205 at 3. Symantec's belated request to divorce the term "anomalous," as used in patents-in-suit, from the computer system usage it originally acknowledged, is simply an attempt to bolster its § 101 defense by obscuring that clear relationship.

information" including "stack frames, function-call arguments [and] other features associated with the data sent to or returned from the called function."). This data is used to create, or "train," a model of function calls, typically through the use of artificial intelligence techniques, to develop rules that distinguish typical program execution from the sort of "anomalous" execution that may indicate an attack. *See id.* at 3:10–6:26, 11:8–18.[4] Once trained, the model of function calls is applied to inspect new (and never-before-seen) programs to identify anomalous function calls, and thus potential attacks. *See, e.g., id.* at 8:60–62.

The '115 and '322 patents also describe sharing models among members of an "application community" so that an attack may be detected early no matter where it begins.[5] *Id.* at 6:37–39. In the event that program behavior is identified as anomalous, the claims provide that the application community can be notified, so that "patches or a signature can be provided to those community members" who would otherwise be "blind to the crafted attack." *Id.* at 7:1–6; *see also* '115 patent at claim 1 ("upon identifying the anomalous function call, notifying an application community that includes a plurality of computers of the anomalous function call"). Providing information about the anomalous function call to members of the application community allows the notified computers to "isolate the portion of the code that caused the fault." '322 patent at 18:46–64. By sharing this information, the patented inventions improve computer functionality in systems in the application community.

[4] The construction of "model of function" calls for the "at least a part/portion of the program."

[5] The Court has construed "Application Community" to mean "[m]embers of a community running the same program or a selected portion of the program." Claim Construction Order, Dkt. No. 123.

Importantly, the Asserted Claims include additional features to make the model more robust. As the patents explain, prior systems used a single model shared by an entire application community. If an attacker obtained the model, the attacker could use the resulting understanding to develop attack software that evades the model. In other words, use of a single model could allow an attacker to "potentially access [the model] and use [it] to craft a mimicry attack." *Id.* at 6:54–56. To avoid this evasion of detection, the inventions of the patents-in-suit claim detection methodologies that randomly select among multiple models, or change and update models through a combination of models created using different computers. *See id.* at 8:15–37, 6:37–53 (describing how these combined models allow distribution of computer workload, and reduce the effects of "concept drift"). These "distinct models" make it more difficult for a potential attacker to craft, for example, "mimicry attack" software, because "attacks need to avoid detection by multiple models"—that may be in use in the application community—"rather than just a single model." *Id.* at 6:61–63.

In short, the '115 and '322 Asserted Claims are far from abstract—the claims describe inventions that include the use of sophisticated models to detect anomalous program executions, and approaches for improving overall security by combining models created on different computers and/or at different times and notifying the application community of specific information regarding anomalous functions. *See id.* at 3:16–19, 3:28–4:8, 8:15–44, 18:46–64. Symantec, glossing over these and other details, oversimplifies the Asserted Claims, reducing them to nothing more than "Executing," "Comparing," and "Identifying." But the teachings of the patents-in-suit, and the Asserted Claims that embody those teachings, provide the blueprint for sophisticated modern intrusion detection systems, including those used by Symantec. Am. Compl., Dkt. No. 12 ¶¶ 95–118.

B. Procedural History

Columbia filed this patent infringement suit more than five years ago on December 5, 2013. Compl., Dkt. No. 1. On December 24, 2013, Columbia filed an Amended Complaint, alleging that Symantec infringed six Columbia patents regarding computer security and intrusion detection. Am. Compl., Dkt. No. 12 ¶ 1. On January 14, 2014, Symantec filed its Answer and Defenses, including a defense of invalidity under 35 U.S.C. § 101. Answer, Dkt. No. 20 ¶ 159.

On November 3, 2014, following claim construction, Columbia and Symantec filed a joint motion for entry of a final judgment of non-infringement, which the District Court entered on November 4, 2014, to permit Columbia to take an immediate appeal on certain claim construction rulings. Dkt. Nos. 123, 146, 149, 150, 151. On February 2, 2016, the Federal Circuit vacated certain portions of the claim construction relating to the Asserted Claims and remanded for further proceedings. *Trs. of Columbia Univ. in the City of New York* v. *Symantec Corp.*, 811 F.3d 1359, 1371 (Fed. Cir. 2016).

On December 5, 2014, Symantec filed petitions requesting institution of *inter partes* review ("IPR") by the Patent Trial and Appeal Board ("PTAB") for, among others, the Asserted Claims. *See* Dkt. No. 158. On June 30, 2016, the PTAB issued final written decisions holding, *inter alia*, that Symantec had failed to demonstrate that the Asserted Claims were unpatentable. Dkt. Nos. 199-22, 199-23. The Federal Circuit, on March 13, 2018, affirmed the IPR decisions in their entirety. *Trs. of Columbia Univ. in the City of New York* v. *Symantec Corp.*, 714 F. App'x 1021, 1022 (Fed. Cir. 2018).

Following the Federal Circuit's decision, the Court reopened the case on August 7, 2018. Dkt. No. 181. On October 5, 2018, Columbia filed, with leave of the Court, a motion for partial summary judgment, Dkt. No. 198, and, on October 22, 2018, Symantec filed a motion for additional claim construction, Dkt. No. 204. Both motions were argued on November 27, 2018. *See* Dkt. No. 234.

On May 24, 2019, Symantec filed this Motion for Judgment on the Pleadings Pursuant to Fed. R. Civ. P. 12(c) and 35 U.S.C. § 101. Dkt. No. 245. On May 30, 2019, the Court stayed briefing on the motion, Dkt. No. 248, which the Court lifted on August 5, 2019, Dkt. No. 263.

III. STANDARD FOR JUDGMENT ON THE PLEADINGS

A motion for judgment on the pleadings is only appropriate if it will not delay trial and the pleadings are closed. Fed. R. Civ. P. 12(c). Rule 12(c) motions are "assessed under the same standards as a motion to dismiss under Rule 12(b)(6)." *Occupy Columbia* v. *Haley*, 738 F.3d 107, 115 (4th Cir. 2013). A 12(c) motion should only be granted where "it appears to a certainty that the nonmoving party cannot prove any set of facts in support of its claim that would entitle it to relief." *Great Am. Ins.* v. *GRM Mgmt., LLC*, No. 3:14-cv-295, 2014 WL 6673902, at *2 (E.D. Va. Nov. 24, 2014) (Lauck, J.) (quoting *Shooting Point, LLC* v. *W.M. Cumming*, 238 F. Supp. 2d 729, 735 (E.D. Va. 2002)). Although courts may consider both the complaint and answer when reviewing 12(c) motions, they may only "take the answer's factual allegations as true to the extent the allegations have not been denied or do not conflict with the factual allegations in the complaint," *id.*, and "must . . . draw all reasonable inferences in favor of the plaintiff," *Brown* v. *Huntington Ingalls, Inc.*, No. 4:13-cv-26, 2013 WL 5591932, at *2 (E.D. Va. July 25, 2013) (quoting *Kensington Volunteer Fire Dep't, Inc.* v. *Montgomery Cty.*, 684 F.3d 462, 467 (4th Cir. 2012)).

When evaluating a 12(c) motion, courts may consider "matters of which the [c]ourt[s] must take judicial notice[] and matters of public record," including records of proceedings that took place in front of other courts or agencies. *Choimbol* v. *Fairfield Resorts,* *Inc.*, No. 2:05-cv-463, 2006 WL 2631791, at *4 (E.D. Va. Sept. 11, 2006); *see also Bland* v. *Doubletree Hotel Downtown*, No. 3:09-cv-272, 2010 WL 723805, at *1 (E.D. Va. Mar. 2, 2010) (listing cases in which courts took notice of court record or documents from agency proceedings).

In evaluating a challenge to validity under § 101, the patents are presumed valid, and the defendant must provide persuasive evidence to overcome that presumption. *Cellspin Soft, Inc.* v. *Fitbit, Inc.*, 927 F.3d 1306, 1319 (Fed. Cir. 2019).

IV. THE ’115 AND ’322 PATENTS ARE DIRECTED TO PATENT-ELIGIBLE SUBJECT MATTER UNDER THE *ALICE* ANALYSIS.

Section 101 of the Patent Act lists the categories of patent-eligible subject matter: “[A]ny new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof.” 35 U.S.C. § 101. “[L]aws of nature, natural phenomena, and abstract ideas” are an “important explicit exception” to the patentable categories. *Mayo Collaborative Servs.* v. *Prometheus Labs., Inc.*, 566 U.S. 66, 70 (2012) (quoting *Diamond* v. *Diehr*, 450 U.S. 175, 185 (1981)); *see also Le Roy* v. *Tatham*, 55 U.S. 156, 175 (1852). However, the Supreme Court has also cautioned courts to “tread carefully in construing [these] exclusionary [categories] lest [they] swallow all of patent law,” *Alice Corp.* v. *CLS Bank Int’l*, 573 U.S. 208, 217 (2014) (citing *Mayo*, 566 U.S. at 71), because “[a]t some level, ‘all inventions . . . embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas,’” *id.* (quoting *Mayo*, 566 U.S. at 71). Even if an invention involves an abstract concept, “‘[a]pplication[s]’ of such concepts ‘to a new and useful end’ . . . remain eligible for patent protection.” *Id.* (quoting *Gottschalk* v. *Benson*, 409 U.S. 63, 67 (1972)).

To determine whether a patent is invalid because it claims laws of nature, natural phenomena, or abstract ideas, the Supreme Court has established a two-step analysis. *See id.* at 217–24. Courts must first “determine whether the claims at issue are directed to [a] patent-ineligible concept[].” *Id.* at 217. If so, the second step asks courts to “search for an ‘inventive concept’” that is “sufficient to ‘transform’ the claimed abstract idea into a patent-eligible application.” *Id.* at 217, 221 (quoting *Mayo*, 566 U.S. at 72). Here, as shown below, consideration of the Asserted Claims at each step independently confirms that they are patent-eligible, and not invalid.

A. The Asserted Claims Are Not Directed to an Abstract Idea Because the Inventions Improve Computer Functionality.

Asking “whether the claims at issue are directed to [a] patent-ineligible concept,” *Alice*, 573 U.S. at 217, requires more than simply asking whether the claims merely involve patent-ineligible concepts, such as an abstract idea, because “all inventions at some level” involve such concepts, *Mayo*, 566 U.S. 71. Instead, the step one inquiry requires a determination of whether the claim at issue—“considered in light of the specification” and “based on . . . ‘[its] character as a whole’”—is “directed to excluded subject matter.” *Enfish, LLC* v. *Microsoft Corp.*, 822 F.3d 1327, 1335 (Fed. Cir. 2016) (quoting *Internet Patents Corp.* v. *Active Network, Inc.*, 790 F.3d 1343, 1346 (Fed. Cir. 2015)). The focus of step one is on whether the claims are “directed to” patent-ineligible concepts.

In *Alice*, the Supreme Court suggested that claims “purport[ing] to improve the functioning of the computer itself,” *Alice*, 573 U.S. at 225, or that “improve[] an existing technological process” are patentable, *id.* at 223–25. Inventions covering improvements to computer functionality are not “directed to” patent-ineligible concepts, or to “abstract ideas.” Since *Alice*, the Federal Circuit has repeatedly cited this principle and found that claims which improve computer functionality, like those here, are patentable over a § 101 challenge. As stated by the Federal Circuit, a claim is not directed to an abstract idea, and thus is patentable, if its focus “is on the specific asserted improvement in computer capabilities” rather than on an “‘abstract’ idea for which computers are invoked merely as a tool." *Enfish*, 822 F.3d at 1336; *see also Finjan*, 879 F.3d at 1303–06 (finding software innovations for malware detection patentable as "an improvement in computer functionality"). Simply put, § 101 does not prohibit claims, like the Asserted Claims, that "are directed to a specific improvement to the way computers operate." *Enfish*, 822 F.3d at 1336.

1. Symantec's Motion Should Be Rejected Because It Fails Under the Federal Circuit's Controlling Decision in *Finjan*—a Decision Symantec Ignores.

Symantec essentially ignores the *Alice*/*Enfish* clear distinction between patent-eligible improvements in computer functionality and patent-ineligible abstract ideas. Even more remarkably, Symantec fails to discuss, or even mention, *Finjan*, a Federal Circuit case affirming that software claims directed to a "behavior-based virus scan"—subject matter very similar to the Asserted Claims—constituted "an improvement in computer functionality" and were thus patentable. Although the Asserted Claims disclose valuable technology different from that in *Finjan*, the essential subject matter that the Asserted Claims are directed to is strikingly similar for purposes of § 101: improvement of computer functionality through enhanced, more sophisticated "behavior-based" malware detection.

The Federal Circuit's controlling holding in *Finjan*, standing alone, defeats Symantec's motion. In *Finjan*, the court examined the following claim:

1. A method comprising:
receiving by an inspector a Downloadable;
generating by the inspector a first Downloadable security profile that identifies suspicious code in the received Downloadable; and
linking by the inspector the first Downloadable security profile to the Downloadable before a web server makes the Downloadable available to web clients.

879 F.3d at 1303. The claimed method was comprised of, first, inspecting a downloadable—a downloaded computer program—using a "behavior-based virus scan" to identify whether the code

"performs potentially dangerous or unwanted operations," and, second, using a security profile to notify users of what was found. *Id.* at 1303–04. The Federal Circuit found the invention patentable because it "enable[d] a computer security system to do things it could not do before." *Id.* at 1305. The invention improved computer functionality because a "behavior-based" scan could "analyze a downloadable's code" to determine what operations it performed and "protect against previously unknown viruses." *Id.* at 1304. Further, the security profile "allow[ed] the system to accumulate and utilize newly available, behavior-based information about potential threats." *Id.* at 1305. The Federal Circuit also found the *Finjan* claim patentable despite the fact that its underlying premise was a comparison of operations in the downloadable against "hostile or potentially hostile operations" known to the claimed "inspector" to identify those that were potentially dangerous or unwanted. *See id.* at 1304.

Finjan controls the result of Symantec's motion, and the Asserted Claims clearly are patentable. Similar to *Finjan*, the Asserted Claims describe methods to analyze the behavior of a program—as exemplified by function calls—to determine if the program performs potentially dangerous or unwanted operations and, thus, may be under attack. As in *Finjan*, the inventions of the Asserted Claims protect against previously unknown viruses, prevent attackers from evading security, and, by communicating anomalous function calls to the application community, allow the accumulation and utilization of behavior-based information about new threats. *See, e.g.*, '322 patent at 3:52–56. Moreover, *Finjan* directly contradicts Symantec's assertions that the Asserted Claims are unpatentable because they involve a "compare-and-identify process" or because "[t]he basic premise of the asserted claims is to compare a function call (data) to a model of function calls (model of data) and to potentially identify the function call as anomalous based on the comparison." *See* Symantec Br. at 11. Symantec raised essentially the same arguments in *Finjan*. The Federal Circuit rejected them. Respectfully the Court should do the same here.

Of course, *Finjan* is not the only case to consider whether a claimed software invention is patentable because it "constitutes an improvement in computer functionality." The principle that inventions that claim improvements in computer capabilities are not directed to abstract ideas has been repeatedly applied by the Federal Circuit in several recent decisions, all of which Symantec ignores.

In addition to *Enfish* and *Finjan*, the Federal Circuit held patentable claims directed to improvements in computer functionality in, for example, *Core Wireless Licensing S.A.R.L.* v. *LG Electronics, Inc.*, 880 F.3d 1356, 1362–63 (Fed. Cir. 2018). In *Core Wireless*, the Federal Circuit found patentable software that analyzed and summarized program menu content for display on smaller screens, because claim language "indicat[ed] that the claims are directed to an improvement in the functioning of computers, particularly those with small screens." *Id.* at 1363; *see also Data Engine Techs. LLC* v. *Google LLC*, 906 F.3d 999, 1007–11 (Fed. Cir. 2018) (software that improved accessibility of spreadsheet functions is patentable under § 101). And, in *Ancora Technologies, Inc.* v. *HTC America, Inc.*, 908 F.3d 1343 (Fed. Cir. 2018), the Federal Circuit found patentable claims directed to computer security software that limited a computer's ability to run unauthorized programs. The claimed invention compared information provided by the program against a "license record" stored in a particular location in the computer's memory. *Id.* at 1345. Particularly notably, the claimed invention in *Ancora* improved computer security by comparing and identifying data and was patentable, which is contrary to the entire premise of Symantec's motion. *See* Symantec Br. at 2.

As the Federal Circuit has repeatedly recognized in words directly applicable here, "[i]mproving security . . . can be a non-abstract computer-functionality improvement if done by a specific technique that departs from earlier approaches to solve a specific computer problem." *Ancora*, 908 F.3d at 1348; *see also Finjan*, 879 F.3d at 1305 (Claims were patentable because they "recite specific steps—generating a security profile that identifies suspicious code and linking it to a downloadable—that accomplish the desired result.").

The Asserted Claims "considered in light of the specification" and "based on . . . 'their character as a whole,'" *Enfish*, 822 F.3d at 1335 (quoting *Internet Patents*, 790 F.3d at 1346), recite specific steps and a technique for improving computer security that departs from earlier approaches. The Asserted Claims require running a program in an emulator, or modifying the program itself, to identify the specific aspects of that program (function calls) whose behavior, the inventors found, could indicate malicious software or an attack. The Asserted Claims also require the use of a "model of function calls"—either randomly chosen or created by combining other models created on different computers—to identify threats, and further require notifying other users about those threats. *See supra* Part II.A. Together, the specific steps set out in the Asserted Claims enable a computer to do things it could never do before. For all the reasons addressed by the Federal Circuit in the cases cited above, the Asserted Claims are directed to patent eligible subject matter. *See Finjan*, 879 F.3d at 1305.

2. <u>Symantec Relies on an Improper, Overly Broad Abstraction of the Asserted Claims and Inapplicable Federal Circuit Precedent</u>.

Symantec's motion ultimately depends on both ignoring the controlling Supreme Court and Federal Circuit cases discussed above and oversimplifying into unrecognizability the inventions of the '115 and '322 patents to be no more than "comparing and identifying data" with an "Executing Step," a "Comparing Step," and an "Identifying Step." Symantec Br. at 2.

Symantec then compares its oversimplified version of the Asserted Claims—intentionally designed to fail the § 101 analysis by ignoring the teachings of the common specification and contradicting the instructions of *Alice* and other § 101 cases—to very different claims having nothing to do with improvements in computer functionality. *See* Symantec Br. at 11–16. Based on this counterfactual set-up, Symantec unremarkably (but wholly incorrectly) concludes that the Asserted Claims are unpatentable.

Symantec's approach, with its self-ordained conclusion, is entirely wrong. Symantec's oversimplification of the Asserted Claims is exactly what the Federal Circuit has said the courts may *not* do: "describing the claims at such a high level of abstraction and untethered from the language of the claims [which] all but ensures" that a claim will be found to be directed to an abstract idea. *Enfish*, 822 F.3d at 1337; *see also Thales Visionix Inc.* v. *United States*, 850 F.3d 1343, 1347 (Fed. Cir. 2017) ("We must therefore ensure at step one that we articulate what the claims are directed to with enough specificity to ensure the step one inquiry is meaningful."); *McRO, Inc.* v. *Bandai Namco Games Am. Inc.*, 837 F.3d 1299, 1313 (Fed. Cir. 2016) ("We have previously cautioned that courts 'must be careful to avoid oversimplifying the claims' by looking at them generally and failing to account for the specific requirements of the claims." (quoting *In re TLI Commc'ns LLC Patent Litig.*, 823 F.3d 607, 611 (Fed. Cir. 2016))); *Visual Memory LLC* v. *NVIDIA Corp.*, 867 F.3d 1253, 1259 (Fed. Cir. 2017) (rejecting defendant's characterization of claims as directed to the "abstract idea of categorical data storage" and instead finding them directed to improved computer memory system). To avoid over-abstraction, the full language of the claims, as construed by the court, must be considered, as well as the manner in which the invention is described in the patent's specification. *See Enfish*, 822 F.3d at 1337 (relying on claim language and the teachings of the specification to find the claims were not directed to an abstract idea); *Core Wireless*, 880 F.3d at 1362–63 (same).

Symantec then compares its oversimplification of the Asserted Claims to wholly unrelated claims that have nothing to do with improvements in computer functionality. *See* Symantec Br. at 11–16. For example, Symantec relies on an out-of-context statement in the unpublished decision in *Intellectual Ventures I LLC* v. *Erie Indemnity Co.*, 711 F. App'x 1012, 1015 (Fed. Cir. 2017), to assert that any claim directed to the identification of a digital file with particular characteristics is directed to an abstract idea. *See* Symantec Br. at 11–12. But that is not remotely what the Federal Circuit held. The patent in *Intellectual Ventures I* claimed "a computerized solution to a longstanding problem that exists outside of computers: identifying and categorizing illicit files," including illegal or pornographic matter "the possession of which might subject an individual or organization to liability." 711 F. App'x at 1014–15 (quoting *Intellectual Ventures I LLC* v. *Erie Indem. Co.*, 200 F. Supp. 3d 565, 575 (W.D. Pa. 2016)). The claims were "not directed to an improvement in the way computers operate," *id*. at 1016, but simply "purport[ed] to accelerate the process of finding errant files and to reduce error," *id*. at 1017. The Federal Circuit held that, absent any improvement in computer functionality itself, "speed and accuracy increases stemming from the ordinary capabilities of a general-purpose computer 'do[] not materially alter the patent eligibility of the claimed subject matter.'" *Id*. (quoting *Bancorp Servs., L.L.C.* v. *Sun Life Assur. Co. of Canada (U.S.)*, 687 F.3d 1266, 1278 (Fed. Cir. 2012)). A simple reading of *Intellectual Ventures* and the claims here confirm the case is wholly inapplicable:

here, the Asserted Claims clearly *are* directed to improving the way computers operate, and do not simply speed up a business practice that might otherwise be done by hand.[6]

Content Extraction & Transmission LLC v. *Wells Fargo Bank, National Association*, 776 F.3d 1343 (Fed. Cir. 2014), another case on which Symantec relies, *see* Symantec Br. at 12–13, is likewise inapplicable. The claims in *Content Extraction* were directed to the use of a scanner to extract certain data from hard-copy documents (contracts), which were then stored in memory. *See Visual Memory*, 867 F.3d at 1260 (discussing *Content Extraction*). In essence, the invention in *Content Extraction* was *the use of a computer* to review contracts and summarize the relevant details; the claims simply implemented a common business practice "on a computer using conventional computer activity." *See id.* (quoting *Enfish*, 822 F.3d at 1338). The claims in *Content Extraction* were unpatentable because they "were not directed to an improvement in computer functionality." *Id.* (noting that the lack of such an improvement "separate[d] the claims" in *Content Extraction* from the patent-eligible claims at issue in *Visual Memory*).

In sum, in a legally correct § 101 analysis,[7] there is a critical difference between claimed technology that merely *uses a computer* to perform a routine task (which may be patent-

[6] Symantec incorrectly suggests that "[t]he [A]sserted [C]laims can be performed manually." *See* Symantec Br. at 19. Symantec fails to explain, *inter alia*, how the limitation that the necessary function calls be extracted from a program running in an emulator—in other words, the behavioral analysis on which the claimed methods are based—might be carried out manually.

[7] Symantec relies on other inapplicable cases, rather than Federal Circuit cases addressing patentability of malware detection inventions. The claims in *Fairwarning IP, LLC* v. *Iatric Systems, Inc.* (discussed in Symantec Br. at 13–14) were "not directed to an improvement in the way computers operate" but instead "merely implement[ed] an old practice in a new environment" by *using a computer* to ask the same questions "that humans in analogous situations detecting fraud have asked for decades, if not centuries." 839 F.3d 1089, 1094–95 (Fed. Cir. 2016). In *Intellectual Ventures I LLC* v. *Symantec Corp.*, the claims were directed to email-filtering software, which merely applied the "well-known idea" of "look[ing] at an envelope and discard[ing] certain letters, without opening them, . . . based on characteristics of the mail" to "the particular technological environment of the internet." 838 F.3d 1307, 1314 (Fed. Cir. 2016) (quoting *DDR Holdings, LLC* v. *Hotels.com, L.P.*, 773 F.3d 1245, 1259 (Fed. Cir. 2014)). Thus,

ineligible) and claimed technology that improves computer functionality (which is patent-eligible). Symantec glosses over this distinction by improperly ignoring all of the details in the common specification, oversimplifying the Asserted Claims, and then improperly comparing that oversimplification to claimed technology that merely uses a computer to perform a routine task. Properly grounded in the common specification and a proper analysis, the Asserted Claims fall within *Finjan* and the many other controlling cases holding that patent claims directed to technology that improves computer functionality are patent-eligible. The Court should rule, as a matter of law, that the Asserted Claims are not directed to abstract ideas and deny Symantec's motion.

B. Step Two of the *Alice* Analysis at a Minimum Raises Questions of Material Fact that Preclude Judgment on the Pleadings.

The Court need not reach step two of the *Alice* analysis for the reasons discussed above. *See Finjan, Inc.* v. *Blue Coat Sys., Inc.*, 879 F.3d 1299, 1306 (Fed. Cir. 2018) ("The idea is non-abstract and there is no need to proceed to step two of *Alice*."); *Thales Visionix Inc.* v. *United States*, 850 F.3d 1343, 1349 (Fed. Cir. 2017) (same). To the extent the Court does consider step two, as shown below the claims contain limitations that were hardly routine or conventional. At a minimum step two raises questions of fact that cannot be resolved on a motion for judgment on the pleadings, and thus also independently requires denial of Symantec's motion. *See Berkheimer* v. *HP Inc.*, 881 F.3d 1360, 1370 (Fed. Cir. 2018) (finding that "fact questions created

the inventions in *Intellectual Ventures I*, like those in all the cases on which Symantec relies, "*use[d] generic computers* to perform generic computer functions" and, unlike the Asserted Claims, did not "improve the functioning of the computer itself." *Id.* at 1315 (emphasis added) (quoting *Alice*, 573 U.S. at 225); *see also Elec. Power Grp., LLC* v. *Alstrom S.A.*, 830 F.3d 1350 (Fed. Cir. 2016) (distinguishing *Enfish* claims because "the focus of the [*Electric Power Group*] claims is not on such an improvement in computers as tools, but on certain independently abstract ideas that use computers as tools") (cited in Symantec Br. at 11).

by the specification's disclosure" at step two made summary judgment "improper"); *Cellspin Soft, Inc.* v. *Fitbit, Inc.*, 927 F.3d 1306, 1318 (Fed. Circ. 2019) ("[F]actual disputes about whether an aspect of the claims is inventive may preclude dismissal at the pleadings stage under § 101.").

At step two of the *Alice* analysis, the Court must "consider the elements of each claim both individually and 'as an ordered combination' to determine whether the additional elements 'transform the nature of the claim' into a patent-eligible application." *Alice*, 573 U.S. at 217 (quoting *Mayo*, 566 U.S. at 78–79). Put differently, a claim that is "directed to" an abstract idea can nevertheless be patent-eligible if the claim includes something more than "'well-understood, routine, conventional activit[ies]' previously known to the industry," *i.e.*, an "inventive concept." *Id.* at 225 (quoting *Mayo*, 566 U.S. at 79–80). "The question of whether a claim element or combination of elements is well-understood, routine and conventional . . . is a question of fact," and "[t]he mere fact that something is disclosed in a piece of prior art, for example, does not mean it was well-understood, routine, and conventional." *Berkheimer*, 881 F.3d at 1368–69.[8]

Here, at least two elements of the Asserted Claims—"a model of function calls for the at least a [part/portion] of the program" (based on randomly selected or combined models), and the "application community"—were not well-understood, routine, or conventional, and offer "inventive concept[s]" that would transform an otherwise abstract idea into patent-eligible subject matter. *See Alice*, 573 U.S. at 221. At a minimum, the common specification of the patents establishes that whether these claim elements were well-understood, routine, and conventional raises issues of material fact that make judgment on the pleadings improper. *See Berkheimer*, 881

[8] For this reason, Symantec's reliance on prior art, *see* Symantec Br. at 15 n.9, in addition to being improper on a motion for judgment on the pleadings, does not establish that the elements of the Asserted Claims were well-understood, routine, and conventional.

F.3d at 1370 ("[O]n this record summary judgment was improper, given the fact questions created by the specification's disclosure."); *see also Symantec Corp.* v. *Zscaler, Inc.*, No. 17-cv-4426, 2018 WL 3537201, at *3 (N.D. Cal. July 23, 2018) ("In sum, under *Berkheimer* improvements in the specification captured in the claims *may* create fact questions which preclude finding a patent ineligible as a matter of law."); *cf. TriPlay, Inc.* v. *WhatsApp Inc.*, No. 13-cv-1703, 2018 WL 1479027, at *8 (D. Del. Mar. 27, 2018) ("Unlike, for instance, the claims involved in *Ber[k]heimer*, the specification here is silent as to what the specific claimed improvement is, how it differs from the prior art, or how any inventive feature, alone or as an ordered combination, is used in an unconventional manner."), *aff'd per curiam*, 771 F. App'x 492 (Fed. Cir. 2019).

1. The "Model of Function Calls" Element, Selected Randomly from Multiple Models or Created by Combining Models, Provides an "Inventive Concept."

The requirement in the Asserted Claims for the use of a "model of function calls" that must be created or chosen in a particular manner presents an "inventive concept" that would render claims "directed to" an abstract idea patent-eligible subject matter. This element does not "merely require generic computer implementation," *see Alice*, 573 U.S. at 221, but is itself a specific improvement in computer technology. As the complaint alleges, the model disclosed and claimed in the patents "can be trained to analyze large amounts of data about various kinds of files and generate detection models that far more effectively distinguish normal computer operation from anomalous or malicious behaviors" and constituted an "advancement[]" over prior technology. Am. Compl., Dkt No. 12, ¶ 15. *Compare Cellspin Soft*, 927 F.3d at 1317–18 (At step two, complaint's "specific, plausible factual allegations about why aspects of its claimed inventions were not conventional" precluded dismissal under Rule 12.).

At the time of the patented inventions, well-understood, routine, and conventional models faced at least two technological problems. First, computers used a single model for malware detection that, if discovered, risked an attacker designing around the model. *See* '115 patent at 6:48–50 ("Model sharing can result in one standard model that an attacker could potentially access and use to craft a mimicry attack."). The "model of function calls" element in the Asserted Claims addresses this problem by offering two specific (and independent) approaches for developing "unique and diversified models" for more "resistant" detections and more "efficient" systems. *Id.* at 6:57–59. One approach is to randomly select a model, or portion thereof, from "a plurality of different models." *See, e.g.*, *id.* at claims 9, 10. Another approach is to create a "combined model from at least two models created using different computers." *See, e.g.*, *id.* at claim 23. Both approaches result in more "resistant" detections, because, from the attacker's perspective, "attacks may need to avoid detection by multiple models, rather than just a single model." *Id.* at 6:55–57. And both approaches simultaneously create more "efficient" computer functionality, because, from the user's perspective, only one model (or portions thereof) out of multiple models is used on, or created by, any particular computer. *See id.* at 6:57–67. Each approach individually provides an "inventive concept" that "not only has the advantage of being more resistant to mimicry attacks, but also may be more efficient" for the computer. *Id.* at 6:57–59.

The second technical problem solved by the inventors was that, over time, "previously learned model[s]" would "no longer accurately reflect" the characteristics for which they modeled. '115 patent at 7:61–65. This technical problem is known as "concept drift." *Id.* at 7:66. Before the disclosure of the "model of function calls" element by the inventors, the solution to the concept-drift problem was to "retire[] or expunge[], and replace[]" the old model with a new one. *Id.* at 8:15–21. The Asserted Claims disclosed a better, inventive, more effective way of addressing concept drift. Rather than expunge the old model, the "model of function calls" allowed for an update of the old model into a new one sufficient to make "attacks far more difficult to achieve." *Id.* at 8:45–48. This "concept of model updating" obviously enhanced detection by updating an old model, but also simultaneously achieved improved functionality: for example, "rather than computing two models by the same device for a distinct application, two distinct models may be computed by two distinct instances of an application by two distinct devices." *Id.* at 8:32–40. This solution to "concept drift" thus improves computer functionality, both in terms of detection and processing.

In offering inventive solutions to the technical problems described above, the "model of function calls" element, whether selected randomly from multiple models or created through a combining of models created using different computers, provides an inventive concept that renders an otherwise abstract idea patent-eligible subject matter. At the very least, whether the "model of function calls" element was well-understood, routine, or conventional raises questions of material fact that preclude judgment on the pleadings.

2. The Ordered Combination of the "Model of Function Calls" and "Application Community" Elements Provides an "Inventive Concept."

Just as an inventive concept can be found in an individual claim element, as shown above, "an inventive concept can be found in the non-conventional and non-generic *arrangement* of known, conventional pieces." *Bascom Glob. Internet Servs., Inc.* v. *AT&T Mobility LLC*, 827 F.3d 1341, 1350 (Fed. Cir. 2016) (emphasis added). The arrangement of the "model of function calls" element and the "application community" element in each of the Asserted Claims also provides an "inventive concept" that overcame problems in then-existing cybersecurity systems.

At the time of the inventions claimed in the Asserted Claims, existing models required a significant amount of time to create or "learn." Before the Asserted Claims, "a single application instance [might] have to be run many times (e.g., thousands of times) in order to compute an application profile or model." '322 patent, 7:56–58. This created a resource problem for computers that hindered their performance. The use of an "application community" in connection with a "model of function calls" solved this problem by sharing the computational load. As described in the common specification of the patents, "models are shared among many members of a community running the same application (referred to as an 'application community')." *Id.* at 6:37–39. By sharing the computational load among an application community, "the learning of anomaly detection models is relatively quick." *Id.* at 6:39–42.

The ordered combination of the "model of function calls" element and "application community" element further improved computer performance by offering diversified, but comprehensive, protection that was previously unavailable. The Asserted Claims achieve this "inventive concept" by expanding the focus of cybersecurity to a network of computers, or "application community," rather than the well-understood, routine, and conventional unit of a single computer. The combination improved detection and combination performance, because the use of the "application community" allowed for the creation of a "model of function calls" for larger and more complex computer applications. Previously, a single computer would need to dedicate a significant portion of its processing power to analyzing the large quantities of raw data needed to construct a "model of function calls" for large and complex computer applications. But spreading the processing power needed to create such a "model of function calls" across an "application community" required each individual computer in an application community to dedicate only a small portion of its resources to such analysis. As the common specification explains, the application community "enable[d] the rapid acquisition of statistics, and relatively fast learning of an application profile by sharing, for example, aggregate information (rather than the actual raw data used to construct the model)." *Id.* at 6:49–53. This "alleviate[d] monitoring costs, [because,] instead of running a particular application for days at a single site, many (e.g., thousands) replicated versions of the application may be run for a shorter period of time (e.g., an hour) to obtain the necessary models." *Id.* at 9:14–18.

The combination of the "model of function calls" and "application community" elements offers a non-conventional and non-generic arrangement of arguably known, conventional pieces. This is sufficient to meet the step two requirements of the *Alice* analysis or, at the very least, raises questions of material fact that preclude judgment on the pleadings.

3. Symantec Cannot Meet Its Burden of Showing That There Is No Set of Facts That Supports Patent-Eligibility.

The only affirmative evidence Symantec cites for its "step two" analysis is a few lines in the common specification which Symantec selectively edits to remove the innovations the specification discloses. *See* Symantec Br. at 22. However, review of the unedited sentences cited by Symantec demonstrates that, in fact and contrary to Symantec's assertions, the Asserted Claims constitute an improvement to prior existing computer technology. *See* '322 patent, 8:24–27 ("*In this case, according to various embodiments, rather than expunging the old model,* a newly created model can be algorithmically combined with the older model using any of a variety of suitable means.") (emphasis indicating language excluded by Symantec); *id.* at 8:40–44 ("*For example, rather than computing two models by the same device for a distinct application,* two distinct models may be computed by two distinct instances of an application by two distinct devices . . . .") (emphasis indicating language excluded by Symantec). Unedited, these portions of the specification in fact demonstrate why the patented invention is an improvement over prior technologies that required, for example, "expunging the old model" or "computing two models by the same device."

The remainder of Symantec's "step two" analysis focuses on an alleged deficiency in the amount of detail provided in the Asserted Claims. *See* Symantec Br. at 22–23. Symantec argues that the '115 and '322 patent claims fail to describe *how* to carry out the steps of the Asserted Claims. *See id.* (asserting that claims do not describe, *e.g.*, "how to execute a program," or how to create a "model of function calls"). But these issues are simply irrelevant to step two of *Alice*. The question at step two is not whether the claims describe how to practice each claim element individually, but how those elements were used in the invention in a manner that was not well-understood, routine, or conventional to achieve the desired result of the invention. *See Elec. Power Grp., LLC* v. *Alstom S.A.*, 830 F.3d 1350, 1355 (Fed. Cir. 2016) ("Inquiry therefore must turn to any requirements for *how* the desired *result* is achieved.") (second emphasis added); *DDR Holdings, LLC* v. *Hotels.com, L.P.*, 773 F.3d 1245, 1258 (Fed. Cir. 2014) ("[T]he claims at issue here specify how interactions with the Internet are manipulated to yield a desired result . . . ."). Simply put, Symantec's arguments miss the point. Here, the claims disclose, the specification describes, and Columbia's complaint alleges how elements that were not well-understood, routine, or conventional are used together to achieve the desired computer security results, and that is sufficient to meet the second step of the § 101 analysis.

In sum, viewed in the light most favorable to the patent owner and applying the presumption of validity, the Asserted Claims include elements that were not well-understood, routine, or conventional, and show how those elements are used to achieve enhanced computer security. But at a minimum, the common specification of the '115 and '322 patents raises issues of material fact with respect to step two of the *Alice* test that preclude judgment on the pleadings. As noted above, the Court need not reach "step two" to deny Symantec's § 101 defense with prejudice because the Asserted Claims clearly are not directed to an abstract idea, but even if it did, Symantec's motion should still be denied.

V. CONCLUSION

For the foregoing reasons, Symantec's motion for judgment on the pleadings should be denied, and Symantec's § 101 defense should be denied with prejudice as a matter of law.

Dated: August 5, 2019

Respectfully submitted,

/s/ John M. Erbach

Dana D. McDaniel (VSB No. 25419)
John M. Erbach (VSB No. 76695)
SPOTTS FAIN, P.C.
411 East Franklin Street, Suite 600
Richmond, Virginia 23219
Tel.: (804) 697-2065
Fax: (804) 697-2165
dmcdaniel@spottsfain.com
jerbach@spottsfain.com

Garrard R. Beeney (*pro hac vice*)
Stephen J. Elliott (*pro hac vice*)
Dustin F. Guzior (*pro hac vice*)
SULLIVAN & CROMWELL LLP
125 Broad Street
New York, New York 10004
Tel.: (212) 558-4000
Fax: (212) 558-3588
beeneyg@sullcrom.com
elliotts@sullcrom.com
guziord@sullcrom.com

Counsel for Plaintiff The Trustees of Columbia University in the City of New York

CERTIFICATE OF SERVICE

I, the undersigned, do hereby certify that on the 5th day of August, 2019, I will electronically file the foregoing Memorandum in Opposition to Defendant's Motion for Judgment on the Pleadings Pursuant to Fed. R. Civ. P. 12(c) and 35 U.S.C. § 101 using the CM/ECF system, which will then send a notification of such filing (NEF) to all counsel of record.

/s/ *John M. Erbach*
Dana D. McDaniel (VSB No. 25419)
John M. Erbach (VSB No. 76695)
SPOTTS FAIN, P.C.
411 East Franklin Street, Suite 600
Richmond, Virginia 23219
Tel.: (804) 697-2065
Fax: (804) 697-2165
dmcdaniel@spottsfain.com
jerbach@spottsfain.com